UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/782,630	02/19/2004	John Cockerham		5107

7590 06/25/2008

JOHN COCKERHAM
3165 N 36TH AVENUE
HOLLYWOOD, FL 33021

EXAMINER	
DEGA, MURALI K	

ART UNIT	PAPER NUMBER
4176	

MAIL DATE	DELIVERY MODE
06/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/782,630	COCKERHAM, JOHN	
	Examiner	Art Unit	
	MURALI K. DEGA	4176	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) *None* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20040420*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 24, 25, and 28-33 are rejected under 35 U.S.C. 102(b) as being unpatentable by Sixtus (US 5,903,721).

3. With respect to claim 24:

4. Sixtus discloses a system for conducting a purchase transaction over a network, the system comprising a buyer computer, a merchant computer and a clearinghouse computer each connected to the network:

- Merchant computer is adapted to: receive from the buyer computer a purchase transaction request; create a bookmark index, a purchase transaction number specific to the transaction, and a purchase receipt; and send the bookmark index, the purchase transaction number specific

to the transaction, and the purchase receipt to the user computer and send the bookmark index the transaction number to the clearinghouse computer (Abstract, Figs. 1, 2 and 3 and col. 3, ll. 37-42, where the user and the vendor being part of the network and vendor transmitting the transaction information to the trust server for further authentication of the user, a functional equivalent of a clearing house).

- The buyer computer comprises a resident biometric identifier, computer purchaser transaction information and a plurality of authentication datasets of purchaser identifying information (herein collectively, "purchaser registration data"), wherein each authentication dataset is associated with a unique authentication methodology and wherein the buyer computer is adapted to: send a purchase transaction request to the merchant computer; receive from the merchant computer bookmark index, the purchase transaction number specific to the transaction, and the purchase receipt; receive a proffered biometric identifier from the buyer; make a determination whether the proffered biometric identifier matches the resident biometric identifier (Abstract, figs. 1, 2 and 3, where the user initiating a purchase action with a vendor is described, col. 5, ll. 10-27 discussed the use of PIN number stored at the user computer for access control and col. 3, ll. 48-55 discloses the user computer generating authentication number as a function of a unique user registration number,

time stamp and stored user matrix, which is functional equivalent of a unique authentication methodology utilizing purchaser identification data stored in the user computer).

- In the event the proffered biometric identifier matches the resident biometric identifier--generate an authentication identifier, wherein the authentication identifier is associated with a unique authentication methodology; generate a sequence string; insert the authentication identifier at a location within the sequence string determined by the bookmark index; generate the particular one of the plurality of authentication datasets associated with the unique authentication method designated by the authentication identifier; and send the sequence string, the particular one of the plurality of authentication datasets, the transaction number and the purchase receipt to the clearinghouse computer (Col. 5, ll. 10-27 discussed the use of PIN number stored at the user computer for access control and col. 3, ll. 48-55 discloses the user computer generating authentication number as a function of a unique user registration number, time stamp and stored user matrix, which is functional equivalent of a unique authentication methodology utilizing purchaser identification data stored in the user computer, also, abstract discloses communication between user and the trust server of user registration information, which is functional equivalent of a clearinghouse).

- The clearinghouse computer comprises purchaser registration data and is adapted to: locate the authentication identifier in the sequence string using the bookmark index received from the merchant; and apply the unique authentication methodology associated with the authentication identifier to the particular one of the plurality of authentication datasets received from the user computer to authenticate the purchaser; and in the event the application of the unique authentication methodology associated with the authentication identifier to the particular one of the plurality of authentication datasets is successful, authorize the transaction without any purchaser registration data being provided to the merchant (Abstract, discloses receiving the user identification information, purchase information and vendor information and further describes the authentication process using unique user registration number, time stamp and stored user matrix, which is functional equivalent of a unique authentication methodology utilizing purchaser identification data, col. 3, ll. 46-47 and col. 3, ll. 8-9, where authenticating the purchaser and authorizing the purchase transaction without transmitting the user's financial information such as credit card numbers is disclosed, col. 3, ll. 16-19, where data transmission without the use of complex encryption methodology is disclosed).

5. With respect to claim 25:

6. Sixtus discloses the system using internet (Abstract, figs. 1 and 2).

7. With respect to claim 33:

8. Sixtus discloses the system transaction is a purchase of goods or services (Column 4, ll. 50-54 and col. 7, ll. 65-67, where user being interested in goods or services is disclosed).

9. With respect to claim 35:

10. Sixtus discloses a method for authenticating a participant in a transaction conducted over a network:

- Generating a bookmark index at the computer of a first participant and sending the bookmark index to a clearinghouse computer and the computer of a second participant (Abstract, figs. 1, 2 and 5, where plurality of users and vendors is indicated).
- at the computer of the second participant: generating an authentication identifier, wherein the authentication identifier is associated with a unique authentication methodology; generating a sequence string; inserting the authentication identifier at a location within the sequence string determined by the bookmark index; generating the particular one of the plurality of authentication datasets associated with the unique authentication method designated by the authentication identifier; and sending the sequence string and the particular one of the plurality of

authentication datasets to the clearinghouse computer (Col. 5, ll. 10-27 discussed the use of PIN number stored at the user computer for access control and col. 3, ll. 48-55 discloses the user computer generating authentication number as a function of a unique user registration number, time stamp and stored user matrix, which is functional equivalent of a unique authentication methodology utilizing purchaser identification data stored in the user computer, also, abstract discloses communication between user and the trust server of user registration information, which is functional equivalent of a clearinghouse).

11. With respect to claim 36:

12. Sixtus discloses a method for authenticating a participant in a transaction conducted over a network, the method comprising: receiving at a clearinghouse computer a bookmark index from a first participant and a sequence string from a second participant; locating an authentication identifier in the sequence string using the bookmark index received from the first participant; and applying an authentication methodology associated with the authentication identifier to a particular one of the plurality of authentication datasets associated with the second participant; in the event the application of the unique authentication methodology associated with the authentication identifier to the particular one of the plurality of authentication datasets is successful, authenticating the second participant (Abstract, discloses receiving the user identification information, purchase information and vendor information and further

describes the authentication process using unique user registration number, time stamp and stored user matrix, which is functional equivalent of a unique authentication methodology utilizing purchaser identification data, col. 3, ll. 46-47 and col. 3, ll. 8-9, where authenticating the purchaser and authorizing the purchase transaction without transmitting the user's financial information such as credit card numbers is disclosed, col. 3, ll. 16-19, where data transmission without the use of complex encryption methodology is disclosed).

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

15. Claims 1-3, 6-11, 13, 14, 17-22 and 28-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sixtus (US 5903721) in view of Johnson (US 6898577).

16. With respect to claim 1:

17. Sixtus discloses a method for authorizing a purchase transaction between a merchant and a purchaser over a network:

- A user computer sending a purchase request to a merchant computer (Abstract, figs. 1, 2 and 3, where the user initiating a purchase action with a vendor is described).
- The merchant computer, sending transaction data and an identifier indicative of an authentication methodology to the user computer and a clearinghouse computer (Abstract, Figs. 1, 2 and 3 and col. 3, ll. 37-42, where the user and the vendor being part of the network and vendor transmitting the transaction information to the trust server for further authentication of the user, a functional equivalent of a clearing house).
- In the event the proffered biometric identifier and the stored biometric identifier match, at the user computer sending an authentication dataset of purchaser identifying information associated with the authentication identifier and transaction information to the clearinghouse computer (Col. 5, ll. 10-27 discloses the use of PIN number by user and the user gaining access to the trust server only after matching the PIN number and the registration number, and further, abstract, figs. 1 & 2, col. 4, ll. 10-13,

discloses the trust server receiving authentication number and the user network address from the user computer, which is functional equivalent of the claim).

- Whereupon successful authentication of the purchaser, the transaction is authorized by the clearinghouse without any purchaser registration data being provided to the merchant (Abstract, fig. 3, col. 3, ll. 46-47 and col. 3, ll. 8-9, where the trust server which is functional equivalent of a clearinghouse for authentication purposes, authenticating the purchaser and authorizing the purchase transaction without transmitting the user's financial information such as credit card numbers is disclosed).
- Sixtus discloses proffering a biometric identifier to the user computer, wherein the user computer determines whether the proffered biometric identifier and a stored biometric identifier match, in the form of a PIN number to gain access to the user client (Fig. 4B and col. 5, ll. 10-27). Sixtus does not explicitly disclose use of biometric identifier.
- However, Johnson teaches (Abstract, col. 5, ll. 52-55) the use of biometric data such as fingerprints, retinal scan and/ or voice scan. Therefore, it would have been obvious to one of ordinary skills in the art, at the time of invention to have modified the system of Sixtus so as to use biometric identifiers in place of PIN number to gain access to the user computer, in accordance with the teachings of Johnson, for access control, since so

doing could be performed readily and easily by any person of ordinary skill in the art, with neither undue experimentation nor risk of unexpected results.

18. With respect to claim 2:

19. Sixtus discloses the method for authorizing a purchase transaction between a merchant and a purchaser over a network:

- Storing on a user computer purchaser transaction information and a plurality of authentication datasets of purchaser identifying information (herein collectively, "purchaser registration data"), wherein each authentication dataset is associated with a unique authentication methodology (Col. 5, ll. 10-27 discussed the use of PIN number stored at the user computer for access control and col. 3, ll. 48-55 discloses the user computer generating authentication number as a function of a unique user registration number, time stamp and stored user matrix, which is functional equivalent of a unique authentication methodology utilizing purchaser identification data stored in the user computer).
- Storing the purchaser registration data on a clearinghouse computer (Col. 3, ll. 20-24 where user pre-registering with the trust server is disclosed, for the purposes of clearinghouse authenticating the user utilizing the internally stored user registration data).

- Sixtus discloses uniquely associating the purchaser with the purchaser registration data stored on the user computer using a biometric identifier obtained from the purchaser and stored solely on the user computer, using a PIN number stored in the user computer being used to gain access to the user client (Fig. 4B and col. 5, ll. 10-27). Sixtus does not explicitly mention use of biometric identifier.
- However, Johnson discloses (Abstract, col. 5, ll. 52-55) the use of biometric data such as fingerprints, retinal scan and/ or voice scan that are stored in user computer, to gain access to the user computer. Therefore, it would have been obvious to one of ordinary skills in the art, at the time of invention to have modified the system of Sixtus so as to use biometric identifiers in place of PIN number to gain access to the user computer, in accordance with the teachings of Johnson, for access control, since so doing could be performed readily and easily by any person of ordinary skill in the art, with neither undue experimentation nor risk of unexpected results.

20. With respect to claim 3:

21. Sixtus discloses authorizing a purchase transaction between a merchant and a purchaser over a network such as internet (Abstract, figs. 1 and 2).

22. With respect to claims 6-10:

23. Sixtus discloses the above limitations, but does not explicitly disclose claims 6-10. However, Johnson teaches the method for authorizing a purchase transaction between a merchant and a purchaser over a network utilizing biometric identification information such as fingerprint scan, face print scan, retinal scan, palm print scan and/or voice print scan. Sixtus discloses utilization of user identification (Sixtus, abstract, figs. 3, 4A, 4B, 4C and 4D, col. 3, ll. 48-55) but Sixtus does not explicitly mention biometric data. However, Johnson discloses (Abstract, col. 5, ll. 52-55) use of biometric data in user authentication process. Therefore, it would have been obvious to one of ordinary skills in the art, at the time of invention to have modified the system of Sixtus so as to use biometric identifiers in place of PIN number to gain access to the user computer, in accordance with the teachings of Johnson, for authentication, since so doing could be performed readily and easily by any person of ordinary skill in the art, with neither undue experimentation nor risk of unexpected results.

24. With respect to claim 11:

25. Sixtus discloses the method for authorizing a purchase transaction between a merchant and a purchaser over a network, wherein the transaction is a purchase of goods or services (Column 4, ll. 50-54 and col. 7, ll. 65-67, where user being interested in goods or services is disclosed).

26. With respect to claim 13:

27. Sixtus discloses a method for authorizing a purchase transaction between a merchant and a purchaser over a network:

- Storing on a user computer purchaser transaction information and a plurality of authentication datasets of purchaser identifying information (herein collectively, "purchaser registration data"), wherein each authentication dataset is associated with a unique authentication methodology (Col. 5, ll. 10-27 discussed the use of PIN number stored at the user computer for access control and col. 3, ll. 48-55 discloses the user computer generating authentication number as a function of a unique user registration number, time stamp and stored user matrix, which is functional equivalent of a unique authentication methodology utilizing purchaser identification data stored in the user computer).
- Storing the purchaser registration data on a clearinghouse computer (Col. 3, ll. 20-24 where user pre-registering with the trust server is disclosed, for the purposes of clearinghouse authenticating the user utilizing the internally stored user registration data).
- Sending a request to purchase to the merchant computer (Abstract, figs. 1, 2 and 3, where the user initiating a purchase action with a vendor is described).

- From the merchant computer, sending a bookmark index, a purchase transaction number specific to the transaction, and a purchase receipt to the user computer and sending the bookmark index the transaction number to the clearinghouse computer (Abstract, Figs. 1, 2 and 3 and col. 3, ll. 37-42, where the user and the vendor being part of the network and vendor transmitting the transaction information to the trust server for further authentication of the user, a functional equivalent of a clearing house).
- In the event the proffered biometric identifier and the stored biometric identifier match, at the user computer: generating an authentication identifier, wherein the authentication identifier is associated with a unique authentication methodology; generating a sequence string; inserting the authentication identifier at a location within the sequence string determined by the bookmark index; generating the particular one of the plurality of authentication datasets associated with the unique authentication method designated by the authentication identifier; and sending the sequence string, the particular one of the plurality of authentication datasets, the transaction number and the purchase receipt to the clearinghouse computer (Col. 5, ll. 10-27 discussed the use of PIN number stored at the user computer for access control and col. 3, ll. 48-55 discloses the user computer generating authentication number as a

function of a unique user registration number, time stamp and stored user matrix, which is functional equivalent of a unique authentication methodology utilizing purchaser identification data stored in the user computer, also, abstract discloses communication between user and the trust server of user registration information, which is functional equivalent of a clearinghouse).

- At the clearinghouse computer, locating the authentication identifier in the sequence string using the bookmark index received from the merchant; applying the unique authentication methodology associated with the authentication identifier to the particular one of the plurality of authentication datasets received from the user computer to authenticate the purchaser; and in the event the application of the unique authentication methodology associated with the authentication identifier to the particular one of the plurality of authentication datasets is successful, authorizing the transaction without any purchaser registration data being provided to the merchant and without the use of complex mathematical encryption algorithms (Abstract, discloses receiving the user identification information, purchase information and vendor information and further describes the authentication process using unique user registration number, time stamp and stored user matrix, which is functional equivalent of a unique authentication methodology utilizing purchaser identification

data, col. 3, ll. 46-47 and col. 3, ll. 8-9, where authenticating the purchaser and authorizing the purchase transaction without transmitting the user's financial information such as credit card numbers is disclosed, col. 3, ll. 16-19, where data transmission without the use of complex encryption methodology is disclosed).

- Sixtus discloses uniquely associating the purchaser with the purchaser registration data stored on the user computer using a biometric identifier obtained from the purchaser and stored solely on the user computer, in the form of a PIN number stored in the user computer being used to gain access to the user client (Abstract, fig. 4B and col. 5, ll. 10-27). Sixtus does not explicitly mention the use of biometric identifier.
- However, Johnson discloses (Abstract, col. 5, ll. 52-55) the use of biometric data such as fingerprints, retinal scan and/ or voice scan that are stored in user computer, to gain access to the user computer. Therefore, it would have been obvious to one of ordinary skills in the art, at the time of invention to have modified the system of Sixtus so as to use biometric identifiers in place of PIN number to gain access to the user computer, in accordance with the teachings of Johnson, for access control, since so doing could be performed readily and easily by any person of ordinary skill in the art, with neither undue experimentation nor risk of unexpected results.

- Sixtus discloses proffering a biometric identifier to the user computer, wherein the user computer determines whether the proffered biometric identifier and the stored biometric identifier match, as a process of registering with trust server to receive a registration number, use of a PIN number to gain access to the user client (Abstract, fig. 4B and col. 5, ll. 10-27). Sixtus does not explicitly mention the use of biometric identifier.
- However, Johnson discloses (Abstract, col. 5, ll. 52-55) the use of biometric data such as fingerprints, retinal scan and/ or voice scan. Therefore, it would have been obvious to one of ordinary skills in the art, at the time of invention to have modified the system of Sixtus so as to use biometric identifiers in place of PIN number to gain access to the user computer, in accordance with the teachings of Johnson, for access control, since so doing could be performed readily and easily by any person of ordinary skill in the art, with neither undue experimentation nor risk of unexpected results.

28. With respect to claim 14:

29. Sixtus discloses authorizing a purchase transaction between a merchant and a purchaser over a network such as internet (Abstract, figs. 1 and 2).

30. With respect to claims 17-21:

31. Sixtus discloses the above limitations, but does not explicitly disclose claims 17-21. However, Johnson teaches the method for authorizing a purchase transaction

between a merchant and a purchaser over a network utilizing biometric identification information such as fingerprint scan, face print scan, retinal scan, palm print scan and/ or voice print scan (Abstract, figs. 3, 4A, 4B, 4C and 4D, col. 3, ll. 48-55, where utilization of user identification data is substantially discussed, though Sixtus does not explicitly mention biometric data, Johnson discloses (Abstract, col. 5, ll. 52-55) use of biometric data in user authentication process. Therefore, it would have been obvious to one of ordinary skills in the art, at the time of invention to have modified the system of Sixtus so as to use biometric identifiers in place of PIN number to gain access to the user computer, in accordance with the teachings of Johnson, for authentication purposes, since so doing could be performed readily and easily by any person of ordinary skill in the art, with neither undue experimentation nor risk of unexpected results.

32. With respect to claim 22:

33. Sixtus discloses the method for authorizing a purchase transaction between a merchant and a purchaser over a network, wherein the transaction is a purchase of goods or services (Column 4, ll. 50-54 and col. 7, ll. 65-67, where user being interested in goods or services is disclosed).

34. With respect to claims 28-32:

35. Sixtus discloses the above limitations, but does not explicitly disclose claims 28-32. However, Johnson teaches the method for authorizing a purchase transaction between a merchant and a purchaser over a network utilizing biometric identification

information such as fingerprint scan, face print scan, retinal scan, palm print scan and/ or voice print scan (Abstract, figs. 3, 4A, 4B, 4C and 4D, col. 3, ll. 48-55, where utilization of user identification data is substantially discussed, though Sixtus does not specifically disclose biometric data, Johnson discloses (Abstract, col. 5, ll. 52-55) use of biometric data in user authentication process. Therefore, it would have been obvious to one of ordinary skills in the art, at the time of invention to have modified the system of Sixtus so as to use biometric identifiers in place of PIN number to gain access to the user computer, in accordance with the teachings of Johnson, for access control, since so doing could be performed readily and easily by any person of ordinary skill in the art, with neither undue experimentation nor risk of unexpected results.

36. Claims 26, 27 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sixtus as applied to claim 24 above, in view of Livesay (US 7203315).

37. With respect to claims 26 and 27:

38. Sixtus and Johnson disclose all of the above limitations, but does not explicitly disclose wireless network use. Sixtus discloses authorizing a purchase transaction between a merchant and a purchaser over a network such as wireless network and/ or intranet (Col. 4, ll. 65-67, col. 5, ll. 1-5), usage of telephone or fax is disclosed for the purposes of registration and purchase transaction. Sixtus does not explicitly disclose wireless network use. However, Livesay discloses (Col. 6, ll. 36-49) use of any conventional processing device such as wireless phone or PDA being used to establish a connection over a network and further discloses the user device being in a LAN with

access to the internet. Therefore, it would have been obvious to one of ordinary skills in the art, at the time of invention to have modified the system of Sixtus so as to use wireless phone or PDA in place of personal computer, in accordance with the teachings of Livesay, to transact with vendor and clearinghouse, since so doing could be performed readily and easily by any person of ordinary skill in the art, with neither undue experimentation nor risk of unexpected results.

39. With respect to claim 34:

40. Sixtus and Johnson disclose all of the above limitations, but does not explicitly disclose transaction being access and distribution of information. Sixtus discloses the system transaction is an access and distribution of information (Column 4, ll. 50-54 and col. 7, ll. 65-67), where user being interested in goods or services is disclosed. Sixtus does not explicitly disclose the transaction being access and distribution of information. However, Livesay discloses, col. 8, ll. 66-67, electronic goods and services that include software, music and online access services. Therefore, it would have been obvious to one of ordinary skills in the art, at the time of invention to have modified the system of Sixtus so as to buy digital content or gain access to a web site, in place of buying goods or services, in accordance with the teachings of Livesay, in transacting with vendors, since so doing could be performed readily and easily by any person of ordinary skill in the art, with neither undue experimentation nor risk of unexpected results.

41. Claims 4, 5, 12, 15, 16 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sixtus in view of Johnson as applied to claims 1 and 13 above, in view of Livesay (US 7203315).

42. With respect to claims 4 and 5:

43. Sixtus and Johnson disclose all of the above limitations, but does not explicitly disclose wireless network use. Sixtus discloses authorizing a purchase transaction between a merchant and a purchaser over a network such as wireless network and/ or intranet (Col. 4, ll. 65-67, col. 5, ll. 1-5), usage of telephone or fax is disclosed for the purposes of registration and purchase transaction. Sixtus does not explicitly disclose wireless network use. However, Livesay discloses (Col. 6, ll. 36-49) use of any conventional processing device such as wireless phone or PDA being used to establish a connection over a network and further discloses the user device being in a LAN with access to the internet. Therefore, it would have been obvious to one of ordinary skills in the art, at the time of invention to have modified the system of Sixtus so as to use wireless phone or PDA in place of personal computer, in accordance with the teachings of Livesay, to transact with vendor and clearinghouse, since so doing could be performed readily and easily by any person of ordinary skill in the art, with neither undue experimentation nor risk of unexpected results.

44. With respect to claim 12:

45. Sixtus and Johnson disclose all of the above limitations, but does not explicitly disclose the transaction is an access and distribution of information. Sixtus discloses the

method for authorizing a purchase transaction between a merchant and a purchaser over a network, wherein the transaction is an access and distribution of information (Column 4, ll. 50-54 and col. 7, ll. 65-67), where user being interested in goods or services is disclosed. Sixtus does not explicitly disclose the transaction being access and distribution of information. However, Livesay discloses, col. 8, ll. 66-67, electronic goods and services that include software, music and online access services. Therefore, it would have been obvious to one of ordinary skills in the art, at the time of invention to have modified the system of Sixtus so as to buy digital content or gain access to a web site, in place of buying goods or services, in accordance with the teachings of Livesay, in transacting with vendors, since so doing could be performed readily and easily by any person of ordinary skill in the art, with neither undue experimentation nor risk of unexpected results.

46. With respect to claims 15 and 16:

47. Sixtus and Johnson disclose all of the above limitations, but does not explicitly disclose wireless network use. Sixtus discloses authorizing a purchase transaction between a merchant and a purchaser over a network such as wireless network and/ or intranet (Col. 4, ll. 65-67, col. 5, ll. 1-5), usage of telephone or fax is disclosed for the purposes of registration and purchase transaction. Sixtus does not explicitly disclose wireless network use. However, Livesay discloses (Col. 6, ll. 36-49) use of any conventional processing device such as wireless phone or PDA being used to establish a connection over a network and further discloses the user device being in a LAN with

access to the internet. Therefore, it would have been obvious to one of ordinary skills in the art, at the time of invention to have modified the system of Sixtus so as to use wireless phone or PDA in place of personal computer, in accordance with the teachings of Livesay, to transact with vendor and clearinghouse, since so doing could be performed readily and easily by any person of ordinary skill in the art, with neither undue experimentation nor risk of unexpected results.

48. With respect to claim 23:

49. Sixtus and Johnson disclose all of the above limitations, but does not explicitly disclose the transaction being access and distribution of information. Sixtus discloses the method for authorizing a purchase transaction between a merchant and a purchaser over a network, wherein the transaction is an access and distribution of information (Column 4, ll. 50-54 and col. 7, ll. 65-67), where user being interested in goods or services is disclosed. Sixtus does not explicitly disclose the transaction being access and distribution of information. However, Livesay teaches, col. 8, ll. 66-67, electronic goods and services that include software, music and online access services. Therefore, it would have been obvious to one of ordinary skills in the art, at the time of invention to have modified the system of Sixtus so as to buy digital content or gain access to a web site, in place of buying goods or services, in accordance with the teachings of Livesay, in transacting with vendors, since so doing could be performed readily and easily by any person of ordinary skill in the art, with neither undue experimentation nor risk of unexpected results.

Conclusion

50. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Johnson, Richard (US 6,529,885) – A system and method for directory-authenticated electronic transactions
- Kravitz, David (US 6,029,150) – Payment and transactions in electronic commerce system.

51. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MURALI K. DEGA whose telephone number is (571) 270-5394. The examiner can normally be reached Monday to Thursday 7.30 to 5.00 ET.

52. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jerry O'Connor can be reached on (571) 272-6787. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

53. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or (571) 272-1000.

/M. K. D./
Examiner, Art Unit 4176
June 19, 2008

/Gerald J. O'Connor/
Supervisory Patent Examiner
Group Art Unit 4176